PATENT ABSTRACTS OF JAPAN

(11)Publication number : 06-187511
(43)Date of publication of application : 08.07.1994

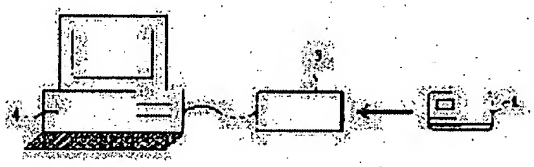
(51)Int.Cl. G06K 17/00
B42D 15/10
B42D 15/10
G09C 1/00
G11B 7/00
G11B 20/10

(21)Application number : 04-356116
(22)Date of filing : 18.12.1992

(71)Applicant : OMRON CORP
(72)Inventor : YODA SHIGERU
KITAJIMA HIROSHI
KOSHIBA YOSHIHITO

(54) INFORMATION RECORDING AND REPRODUCING SYSTEM

(57)Abstract:
PURPOSE: To record even such data for requiring the security on an optical IC card by providing a ciphering key on the IC part of the card when the information is recorded and reproduced at the optical recording part of the card.
CONSTITUTION: The information to be recorded is supplied to the IC part of an IC optical card 1 from a personal computer 4 via an optical IC card reader/ writer 5. The information is ciphered in the card 1 and the information aquired by this ciphering is sent to the reader/writer 5 and the ciphered information is written in the optical recording part of the card 1. The information is ciphered by the secret key of the IC part included in the card 1. Since this key is not viewed from an outside, the ciphered information can be decoded unless only when the secret key is used. The data recorded on the card 1 are read by the computer 4 when the card 1 is put into the reader/writer 5. Then the read information is decoded by the key of the IC part of the card 1.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号

特開平6－187511

(43)公開日　平成６年(1994)７月８日

(51)Int.Cl.[5]	識別記号	庁内整理番号	ＦＩ	技術表示箇所
Ｇ０６Ｋ　17/00		Ａ　7459－5Ｌ		
Ｂ４２Ｄ　15/10	５１１	9111－2Ｃ		
	５２１	9111－2Ｃ		
Ｇ０９Ｃ　1/00		8837－5Ｌ		
Ｇ１１Ｂ　7/00		Ｅ　9195－5Ｄ		

審査請求　未請求　請求項の数７(全　６　頁)　最終頁に続く

(21)出願番号　特願平4－356116

(22)出願日　平成４年(1992)12月18日

(71)出願人　000002945
オムロン株式会社
京都府京都市右京区花園土堂町10番地

(72)発明者　余田　茂
京都府京都市右京区花園土堂町10番地　オムロン株式会社内

(72)発明者　北島　博史
京都府京都市右京区花園土堂町10番地　オムロン株式会社内

(72)発明者　小柴　美仁
京都府京都市右京区花園土堂町10番地　オムロン株式会社内

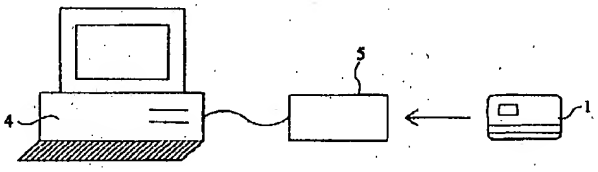
(74)代理人　弁理士　稲本　義雄

(54)【発明の名称】　情報記録再生システム

(57)【要約】

【目的】　守秘性を要求されるデータも光カードに記録できるようにする。

【構成】　光ＩＣカード１のＩＣ部３に暗号化鍵を記憶させ、その光ＩＣカードをＩＣカードリーダライタ５に挿入するとその暗号化鍵がパーソナルコンピュータ４によって読取られ、情報がその暗号化鍵によって暗号化され、光ＩＣカード１に記録される。



1

【特許請求の範囲】
【請求項１】　光ＩＣカードを使用した情報記録再生システムにおいて、
前記光ＩＣカードの光記録部に記録再生する際の暗号化の鍵をそのカードのＩＣ部に持つことを特徴とする情報記録再生システム。
【請求項２】　請求項１に記載の光ＩＣカードを使用した情報記録再生システムにおいておいて、
暗号化の鍵を前記光ＩＣカードをアクセスする情報記録再生装置内に持つことを特徴とする情報記録再生システム。
【請求項３】　請求項１または請求項２に記載の光ＩＣカードを使用した情報記録再生システムにおいて、
前記光ＩＣカード内の暗号化鍵と同じ暗号化鍵をアプリケーション提供者側のシステムに有することを特徴とする情報記録再生システム。
【請求項４】　請求項１乃至請求項３において、
光記録部にセキュリティレベルを持ち、そのセキュリティレベルのうち少なくとも一部は情報を記憶する光ＩＣカードに有する暗号化鍵とは別の鍵によってのみ再生できることを特徴とする情報記録再生システム。
【請求項５】　請求項４において、
セキュリティレベルの一部をアクセスする別の鍵がＩＣカードに記録されていることを特徴とする情報記録再生システム。
【請求項６】　請求項４において、
セキュリティレベルの一部をアクセスする別の鍵が受動的な外部記憶メディアに記録されていることを特徴とする情報記録再生システム。
【請求項７】　請求項４において、
セキュリティレベルの一部をアクセスする別の鍵が光カードまたは情報が記録される光ＩＣカードとは別の光ＩＣカードであることを特徴とする情報記録再生システム。
【発明の詳細な説明】
【０００１】
【産業上の利用分野】本発明は、光カードに情報を記録あるいは再生する情報記録再生システムに関する。
【０００２】
【従来の技術】光ＩＣカードはクレジットカード大の形状をしており、そこに光記録部とＩＣ部を備えている。光記録部は２．８ＭＢ程度のデータが記録できるようになっており、記録したデータは消去できないようになっている。一方、ＩＣ部は８ＫＢ程度の記憶容量を有し、記憶したデータは書換可能であるが、守秘性が保たれるという特徴を有している。
【０００３】従って、光記録部には画像のような大容量のデータや、書換えの必要のないものあるいは、書き換えられると困る個人用ＩＤ等の情報、ＩＣ部には書換えの必要なディレクトリ情報や、秘密性の高い個人情報が

2

記録されている。
【０００４】図８はこのカードの構成を示す図であり、光ＩＣカード１は例えばその長手方向に帯状の光記録部２を有し、その光記録部２を外れた部分に、この例では光記録部２の上側にＩＣ部３を有している。光記録部２の一部分をその右側に拡大して示しており、長手方向に設けられた細い帯状のトラッキングトラック２ａに挟まれた帯状のエリアがデータトラック２ｂとなっており、そのデータトラック２ｂの長手方向中心部付近に、一列に配列された複数のピット２ｃが設けられている。
【０００５】ピット２ｃの記録再生方法は光ディスク装置等で公知の方法を用いており、また本発明に直接関係しないので記載を省略する。
【０００６】図９はピット５の記録状態を示す図であり、仮想的なピットセル２ｄの中央にピット２ｃがあればデータの「１」を示し、ピット２ｃがなければ「０」を示すようになっている。また、隣あったデータが「０」のときはその境界にセルフクロック用のピットを置くようにしている。
【０００７】図９の例では「０１００００１」のデータであり、アスキーコードで記録された情報であれば、「Ａ」を示すことになる。
【０００８】
【発明が解決しようとする課題】しかしながら、このようにして記録した光カードは顕微鏡を使用すればピットの配列状態を読み取ることができるので、守秘性を要求されるデータは記録できないと言う課題を有していた。
【０００９】本発明はこのような状況に鑑みてなされたもので、守秘性を要求されるデータも光カードに記録できるようにしたものである。
【００１０】
【課題を解決するための手段】このような課題を解決するために請求項１に記載の光ＩＣカードを使用した情報記録再生システムにおいて、光ＩＣカードの光記録部に記録再生する際の暗号化の鍵をそのカードのＩＣ部に持つことを特徴とする。
【００１１】請求項２に記載の光ＩＣカードを使用した情報記録再生システムは、請求項１に記載の情報記録再生システムにおいて、暗号化の鍵をその光ＩＣカードをアクセスする情報記録再生装置内に持つことを特徴とする。
【００１２】請求項３に記載の光ＩＣカードを使用した情報記録再生システムは、請求項１または請求項２に記載の情報記録再生システムにおいて、光ＩＣカード内の暗号化鍵と同じ暗号化鍵をアプリケーション提供者側のシステムに有することを特徴とする。
【００１３】請求項４に記載の光ＩＣカードを使用した情報記録再生システムは、請求項１乃至請求項３に記載の情報記録再生システムにおいて、光記録部にセキュリティレベルを持ち、そのセキュリティレベルのうち少な

3

くとも一部は情報を記憶する光ＩＣカードに有する暗号化鍵とは別の鍵によってのみ再生できることを特徴とする。

【００１４】請求項５に記載の光ＩＣカードを使用した情報記録再生システムは、請求項４に記載の情報記録再生システムにおいて、セキュリティレベルの一部をアクセスする別の鍵がＩＣカードに記憶されていることを特徴とする。

【００１５】請求項６に記載の光ＩＣカードを使用した情報記録再生システムは、請求項４に記載の情報記録再生システムにおいて、セキュリティレベルの一部をアクセスする別の鍵が受動的な外部記憶メディアに記録されていることを特徴とする。

【００１６】請求項７に記載の光ＩＣカードを使用した情報記録再生システムは、請求項４に記載の情報記録再生システムにおいて、セキュリティレベルの一部をアクセスする別の鍵が光カードまたは情報の記録される光ＩＣカードとは別の光ＩＣカードであることを特徴とする。

【００１７】

【作用】請求項１に記載の光ＩＣカードを使用した情報記録再生システムは、光ＩＣカードのＩＣ部に記憶されている鍵によってその光ＩＣカードに記録される情報が暗号化され、またその鍵を使用して読出しが行われる。

【００１８】請求項２に記載のＩＣ光カードを使用した情報記録再生システムは、請求項１に記載の情報記録再生システムにおいて、その光ＩＣカードに対して情報をアクセスする情報記録装置内に記憶された鍵によって光ＩＣカードに記録される情報が暗号化され、またその鍵を使用して記録された情報の読出しが行われる。

【００１９】請求項３に記載の光ＩＣカードを使用した情報記録再生システムは、請求項１または２に記載の情報記録再生システムにおいて、光ＩＣカードへの情報暗号化が光アプリケーション提供者側システムに記憶された暗号化鍵で行われ、その暗号化鍵は光ＩＣカード内の暗号化鍵と同じ暗号化鍵が使用される。

【００２０】請求項４に記載の光ＩＣカードを使用した情報記録再生システムは、請求項１乃至請求項３に記載の情報記録再生システムにおいて、光記録部にセキュリティレベルを持ち、そのセキュリティレベルのうち少なくとも一部は情報を記憶する光ＩＣカードに有する暗号化鍵とは別の鍵によってのみ再生される。

【００２１】請求項５に記載の光ＩＣカードを使用した情報記録再生システムは、請求項４に記載の情報記録再生システムにおいて、セキュリティレベルの一部がＩＣカードに記録された別の鍵によってアクセスされる。

【００２２】請求項６に記載の光ＩＣカードを使用した情報記録再生システムは、請求項４に記載の情報記録再生システムにおいて、セキュリティレベルの一部が受動的な外部記憶メディア記録された別の鍵によってアクセスされる。

4

【００２３】請求項７に記載の光ＩＣカードを使用した情報記録再生システムは、請求項４に記載の情報記録再生システムにおいて、セキュリティレベルの一部が光カードまたは情報が記録される光ＩＣカードとは別の光ＩＣカードに記録された別の鍵によってアクセスされる。

【００２４】

【実施例】図１は本発明を適用した装置の一実施例を示す構成図であり、パーソナルコンピュータ４はその内部にアプリケーションプログラムおよび光ＩＣカードリーダライタのコントロールプログラムが収納されている。そしてパーソナルコンピュータ４に光ＩＣカードリーダライタ５接続されている。

【００２５】このＩＣカードリーダライタ５は例えば光ＩＣカード１が着脱自在に挿入できるように構成されている。

【００２６】図２はこのように構成された装置による情報の暗号化および復号化の流れを示す図であり、先ずステップ１００に示すように記録する情報をパーソナルコンピュータ４から光ＩＣリーダライタ５を経由して光ＩＣカード１のＩＣ部３に入力する。

【００２７】そして、ステップ１０１に示すように光ＩＣカード１の内部で暗号化し、その結果得られた情報をステップ１０２に示すように光ＩＣカードリーダライタ５に出力し、ステップ１０３に示すように、暗号化された情報を光記録部２に書き込む。

【００２８】このとき情報の暗号化は光ＩＣカード１内に有するＩＣ部３の秘密の鍵によって行われ、ＩＣ部３内の鍵は外部から覗くことができないものであるため、暗号化された情報は鍵無しでは解読できない。

【００２９】光ＩＣカード１の所有者はこの状態でカードを所持するが、この鍵が何であるかは知らないため、光記録部２に記録されている情報をビット列としては解読できても、情報そのものはわからない。

【００３０】光ＩＣカード１に記録されたデータの読み取りはステップ１０４において光ＩＣカード１を光ＩＣカードリーダライタ５に挿入し、パーソナルコンピュータ４によって読み取りを行う。そしてステップ１０５において読み取られた情報をＩＣ部３に入力し、そこで鍵を用いてステップ１０６に示すように復号を行い、ステップ１０７においてパーソナルコンピュータ４に出力表示する。

【００３１】図３は暗号化の具体例を示したものであり、記録する情報が仮にアルファベットの「Ａ」であるとき、ビット列で「ｄ」（０１０００００１）と表される。暗号化の鍵として８ビットの任意のビット列、例えば「Ｋ」（０００１１０１１）を与えると暗号化は「ｄ」と「Ｋ」のイクスクルーシブオア（ＸＯＲ）を取ることによって行われる。

【００３２】その結果のデータ「Ｄ」は（０１０１１０

１０）となり、情報としてはアルファベットの大文字の「Ｚ」を表すことになる。光ＩＣカード１にはこの「Ｚ」が書き込まれるため、元の情報「Ａ」とは異なり、顕微鏡等で光ＩＣカード１の可視情報を読み取っただけでは元のデータが「Ａ」であることがわからない。復号は再生されたデータ「Ｄ」の（０１０１１０１０）と暗号「Ｋ」の（０００１１０１１）のイクスクルーシブオアをとることで、ｄ（０１０００００１）つまり、元の情報「Ａ」を得ることができる。

【００３３】このように、光ＩＣカード１に記録される情報は元の情報と異なり、また暗号化するときの鍵はＩＣ部３の内部にあって外部に出てくることがないため、暗号化の鍵を知らないものにとっては記録されている情報が何であるかを解読することはできない。

【００３４】この例では簡単のために８ビットの鍵を使用したが、ビット数を増やせばよりセキュリティを上げることができる。また、ＤＥＳ（Ｄａｔａ　Ｅｎｃｒｙｐｔ－ｉｏｎ　Ｓｔａｎｄａｒｄ）のような方法を使用すると更にセキュリティを上げることができる。

【００３５】このようにＩＣ部３に暗号化の鍵を持たせることによってセキュリティを上げることができるが、万一このＩＣ部が破損した場合、光記録部２に記録されている情報を解読できなくなっていまい、情報が失われることになる。

【００３６】この場合、光ＩＣカードリーダライタ５内に光ＩＣカード１のＩＣ部３に持つものと同じ鍵を持っていると、このような事故の際も情報が解読できなくなってしまうことはない。また、この場合は不正な光ＩＣカードリーダライタによるＩＣ部３へのアクセスを防止できる。

【００３７】例えば今までに説明した例ではＩＣ部３に与える情報は光ＩＣカード１から読出した情報をそのまま与え、それを暗号化しているが、図３に示すような単純な鍵を使用すると、その入力と出力の関係で、何回か繰り返すうちに鍵が解読される可能性がある。従ってこのアプリケーション用ではない、他のリーダライタを用いれば鍵が解読される恐れがある。

【００３８】しかし、光ＩＣカードリーダライタ５の内部に光ＩＣカード１の内部にあるのと同じ鍵があるとこのような不正な解読を防止できる。また、ＩＣ部３が破損しても迅速にデータの再生が行える。

【００３９】図４は更にセキュリティを向上させる場合の例であり、アプリケーション提供者システム６と端末システム７を通信回線８によって結んだものであり、アプリケーション提供者システム６は光カードリーダライタ６ａ、ターミナル６ｂ、ＣＰＵ６ｃから構成される。端末システム７はパーソナルコンピュータ７ａ、光ＩＣカードリーダライタ７ｂから構成されている。

【００４０】そしてユーザは光ＩＣカード１を光ＩＣカードリーダライタ７ｂに挿入することにより、そこで読

み取られたデータはアプリケーション側提供者システム６に送られそこで管理され、管理された結果が端末システム７に返送され、光ＩＣカード１に書き込まれる。

【００４１】この場合は、アプリケーション提供者システム６にＩＣ部３と同じ鍵を持たせることにより、通信回線８および端末システム７には暗号化した情報しか現れない。もちろん更にＩＣカードリーダライタ６ａに同じ鍵があっても良い。

【００４２】このような例の中で、図５に示すように、光ＩＣカード１の中にセキュリティレベル記録領域９を設け、その領域を秘密でない情報の領域９ａ、端末システム７により読み取れる領域９ｂ、アプリケーション提供者のみ読み取れる領域９ｃに分けている。このようにすると守秘性が高く、かつ広域で迅速なサービスが提供できるシステムを構成できる。

【００４３】このような光ＩＣカードが破損した場合、アプリケーション提供者にのみ読み取れる領域９ｃはアプリケーション提供者に光ＩＣカードを返却しなければ内容がわからないが、それだけに高い守秘性が保たれる。

【００４４】アプリケーション提供者側システム６を持つ場合、図６に示すようにアプリケーション提供者側システム６にＩＣカードリーダライタ６ｄを設け、管理用ＩＣカード６ｅで鍵の管理を行うと、大量の鍵を安全に管理することができる。

【００４５】例えば６４Ｋビットの容量を持つＩＣカードを使うと、６４ビットの鍵を１０００個、すなわち１０００枚の光ＩＣカードの鍵を管理できる。このような構成にすれば例えば顧客種別の管理ができ、また鍵を変更する際も、対応する一つの鍵を変更するだけで可能である。

【００４６】このＩＣカードの代わりに受動的な外部記憶メディア、例えばハードディスクや光磁気ディスクあるいは、フロピーディスク等を使用すると安全性は多少低下するが、更に大量の鍵を容易に管理できる。また、記憶容量が大きいため、長い鍵すなわちビット数の大きな鍵が使用できる。

【００４７】管理用のカード６ｅに光カードや、光ＩＣカードを使用すると、一つのセクタに記録できる記憶容量が実際に使用される光ＩＣカードのセクタサイズと等しくできるため、一つのセクタ長の鍵を使った場合、効率よく管理できる。更に、管理用光ＩＣカードあるいは光カードの場合、図７に示すようにセクタ毎にユーザを変えて記録できまた、記録する際に暗号化して記録できるため、更に安全である。

【００４８】以上のような鍵の管理はアプリケーション提供者システムだけでなく、端末システムにあっても、あるいは端末側だけにあっても良い。また、端末システムそのものがアプリケーション提供者になるときは以上に述べた鍵の管理がそのまま端末システム上に適用でき

7

る。

【００４９】

【発明の効果】以上説明したように本発明は暗号化鍵を使用して光ＩＣカードに記録する情報を暗号化して記録再生するようにしたので、光ＩＣカードに記録された情報を読取ってもそれだけでは真の情報がわからないので守秘性が保たれるという効果を有する。

【図面の簡単な説明】

【図１】本発明の一実施例の構成をを示す構成図である。

【図２】図１の装置の動作を説明するフローチャートである。

【図３】暗号化の一実施例を示す図である。

【図４】第２の実施例の構成を示す構成図である。

【図５】光ＩＣカード内のセキュリティレベルを説明するための図である。

【図６】第３の実施例の構成を示す構成図である。

【図７】管理用光カードに記録されるデータの配列を説明するための図である。

【図８】従来の光カードを拡大した構成を示す図である。

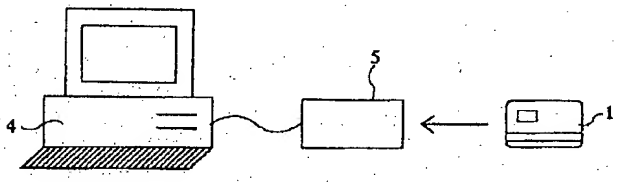
8

【図９】情報とピットとの関係を示す図である。

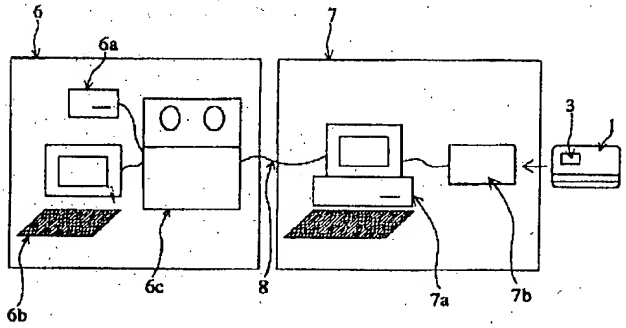
【符号の説明】

１　光ＩＣカード
２　光記録部
２ａ　トラッキングトラック
２ｂ　データトラック
２ｃ　ピット
２ｄ　ピットセル
３　ＩＣ部
４，７ａ　パーソナルコンピュータ
５，７ｂ　光ＩＣカードリーダライタ
６　アプリケーション提供者システム
６ａ　光カードリーダライタ
６ｂ　ターミナル
６ｄ　ＩＣカードリーダライタ
６ｅ　ＩＣカード
７　端末システム
８　通信回線
９　セキュリティレベル記録領域

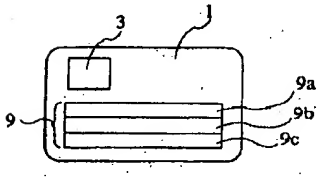
【図１】



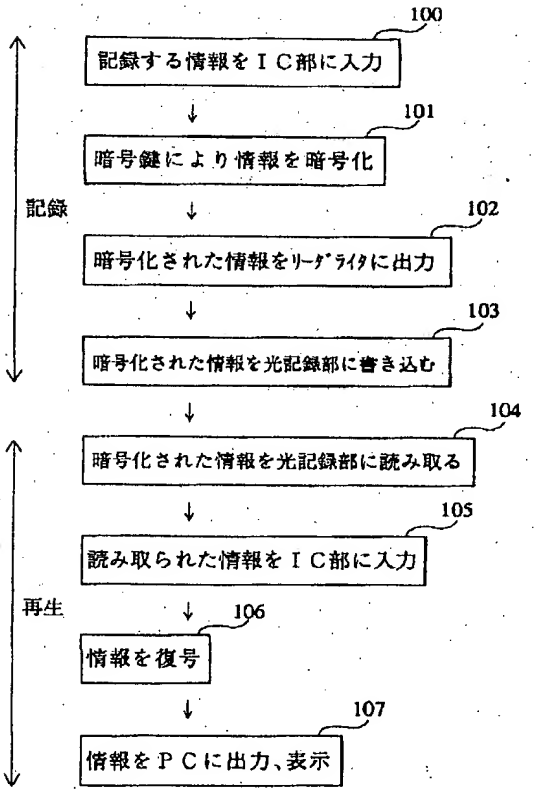
【図４】



【図５】



【図２】



【図３】

情報 “A”　　d(01000001)

鍵　　K(00011011)

暗号化　　d XOR K=D(01011010)

$$\begin{array}{r} d(01000001) \\ \underline{XOR\ K(00011011)} \\ D(01011010) \end{array}$$

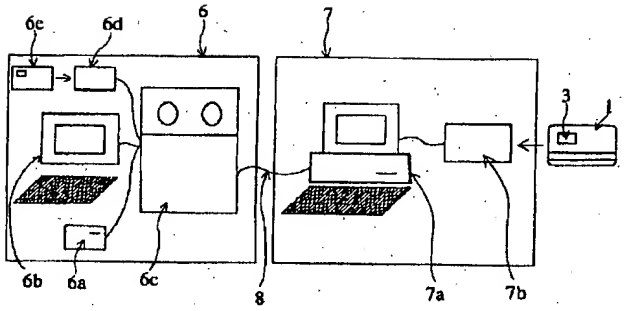
暗号化後情報 “Z”　　D(01011010)

復号　　D XOR K=d(01000001)

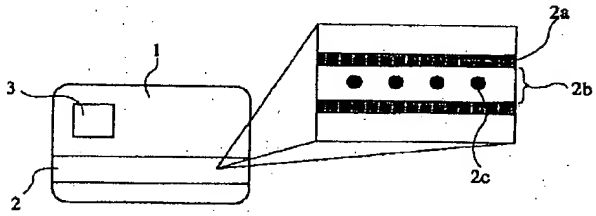
$$\begin{array}{r} D(01011010) \\ \underline{XOR\ K(00011011)} \\ d(01000001) \end{array}$$

復号化後情報 “A”　　d(01000001)

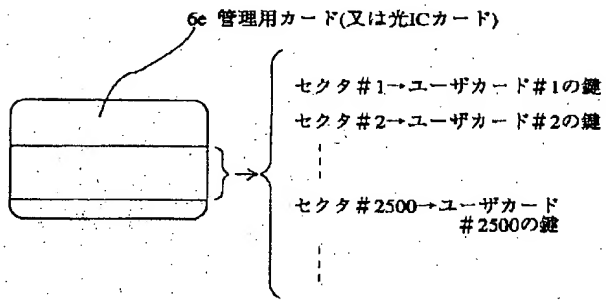
【図６】



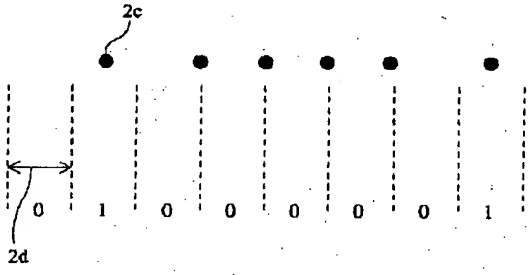
【図８】



【図７】



【図９】



フロントページの続き

(51) Int.Cl.[5]	識別記号	庁内整理番号	F I	技術表示箇所
G11B 20/10		H 7923－5D		